

REMARKS

Claims 1-2, 4-20, 31, 38-41, and 43-48 are pending in the application. With this response, we have added claims 49-51. The application supports the new claims at least at [0038]. No new matter is added by amendment. Reconsideration of the claims, in light of the following remarks, is requested.

The examiner rejected independent claims 1, 38, and 47 under 35 U.S.C. §103(a) as being unpatentable over Jones (5,623,637) in view of Spelman (5,638,445). However, the combination of Jones and Spelman does not disclose or suggest, among other things, a “multi-party secure computation protocol implemented between the client and the server [which] is the only multi-party computation protocol that is implemented in generating the third secret,” as recited in claims 1, 38, and 47.

The examiner first claims that Jones discloses a “multi-party secure computation protocol implemented between the client and the server [which] is the only multi-party computation protocol implemented in generating the third secret” (Office Action, p. 3). However, the examiner then admits that Jones does not disclose:

a multi-party secure computation protocol between a client which has a client secret and the server which has a server secret to compute a third secret from the client secret and the server secret, wherein the protocol is implemented so that the client obtains the third secret and cannot feasibly determine the server secret, and the server cannot feasibly determine the client secret and cannot feasibly determine the third secret

as recited in claims 1, 38, and 47, and goes on to cite Spelman as supposedly disclosing this feature. If Jones does not disclose a multi-party secure computation protocol between a client and a server to compute a third secret (which the examiner admits), then Jones cannot reasonably be construed as disclosing or suggesting that such a protocol is the only protocol that is implemented in computing the third secret, as required by claims 1, 38, and 47.

Spelman does not supply that which is missing from Jones. The examiner cites Spelman as supposedly disclosing:

a protocol wherein the client (merchant) has a client secret (GSO) and the server (merchant acquirer) has a server secret (PI) used to compute a third secret ($C[GSO]_{k1}$; $D[PI]_{k2}$; $E[k1, \dots]_R$; $E[k2, \dots]_R$) from the client and server secret (Office Action, p. 3).

However, neither the “client (merchant)” nor the “server (merchant acquirer)” of Spelman has any involvement in computing $C[GSO]_{k1}$; $D[PI]_{k2}$; $E[k1, \dots]_R$; $E[k2, \dots]_R$, which the examiner treats as the “third secret” of the claims. Instead, Spelman discloses that the consumer performs this computation:

Referring to FIGS. 2A and 3, during the first phase of the protocol, consumer 10 generates four pieces of encrypted data for merchant 20, two of which are derived separately from the GSO and the PI...[C]onsumer 10 separately encrypts the GSO and the PI (col. 5, lines 16-22).

Consumer 10 sends the four pieces of encrypted information (i.e., $C[GSO]_{k1}$, $D[PI]_{k2}$, $E[k1|\text{Merchant name}]_R$, and $E[k2|\text{credit card number}]_R$) to merchant 20 (col. 5, lines 63-64).

In other words, the consumer is actually the only party involved in computing $C[GSO]_{k1}$; $D[PI]_{k2}$; $E[k1, \dots]_R$; $E[k2, \dots]_R$, i.e., the “third secret.” The “client (merchant)” then uses $C[GSO]_{k1}$ to obtain the goods and services order (Fig. 3), and the “server (merchant acquirer)” uses $D[PI]_{k2}$ to obtain the purchase instructions for the order (Fig. 6). This is not a “multi-party secure computation protocol implemented between the client and the server [which] is the only multi-party computation protocol that is implemented in generating the third secret,” as required by claims 1, 38, and 47.

Moreover, there would be no motivation for one of skill in the art to combine the systems of Spelman and Jones in the way the examiner proposes. Because the consumer is the only party involved in computing the so-called “third secret,” Spelman’s merchant and merchant acquirer, which the examiner treats as the “client” and “server” of the claims, play no role in generating the so-called “third secret.” Thus, there would be no motivation for including these components in Jones’s system, even if one wanted to “protect against snooping,” as the examiner proposes (Office Action, p. 4).

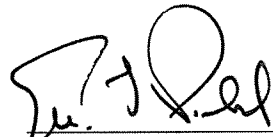
Thus, neither Jones nor Spelman, alone or in combination, render obvious claims 1, 38, or 47, or claims dependent thereon.

In view of the above remarks, applicant believes the pending application is in condition for allowance, and requests the examiner to allow the claims to issue.

A petition for a three-month extension of time accompanies this response, and the Commissioner is authorized to charge the fee required for this extension to Deposit Account No. 08-0219, under Order No. 0081004.00173US2 from which the undersigned is authorized to draw. No other fees are believed to be due at this time. However, please charge any fees, or credit any overpayments, Deposit Account No. 08-0219, under Order No. 0081004.00173US2.

Respectfully submitted,

Dated: October 17, 2007



Eric L. Prah
Registration No.: 32,590
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)